IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TENNESSEE

IN THE MATTER OF THE SEARCH OF A Hewlett Packard Protect Smart Laptop computer, serial number 5CD4470XMM CURRENTLY LOCATED AT FBI Johnson City Resident Agency Office, 2620 Knob Creek Road, Johnson City, Tennessee 37604.

Case No. 2:16-MJ-195

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Bianca L. Pearson being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been so employed since August 12, 2012. I am currently assigned to the Johnson City Resident Agency of the Knoxville field office. As a Special Agent, I am a federal law enforcement officer of the United States as defined by Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure, empowered to enforce criminal laws, make arrests, and serve warrants, pursuant to the Attorney General's Guidelines for Domestic FBI Investigations, I.B.1. and V.A.12., and 18 U.S.C. § 3052. As a Special Agent, I have conducted and participated in a variety of criminal

investigations, including investigations associated with violent crimes against children, organized drug enterprises, bank robberies, fugitives, financial crimes, computer crimes, as well as other violent criminal acts.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a Hewlett Packard Protect Smart Laptop computer, serial number 5CD4470XMM hereinafter the "Device." The Device is currently located at the FBI Johnson City Resident Agency, 2620 Knob Creek Road, Johnson City, Tennessee, 37604.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On September 12, 2016, your affiant and Detectives from Sullivan County Sheriff's Office (SCSO) conducted an undercover operation targeting a Backpage.com advertisement (Post ID: 18684956) that was suspected to be associated with a juvenile runaway (hereinafter referred to as unnamed juvenile "UJ").

7. The undercover operation resulted in the recovery of the UJ and the apprehension and arrest of Brockett Patrick Ian Lang for violating Tennessee Criminal Code Section 39-13-309, trafficking a minor for a commercial sex act.

8. Subsequent to Lang's arrest, he was transported to Sullivan County Detention Center where your affiant and Sullivan County Sheriff's Office Detective Matt Price conducted a custodial interview. Lang was read his Miranda rights by your affiant and waived his Miranda rights by signing a written waiver.

9. Lang admitted that he posts Backpage.com advertisements for the UJ because he has an internet connection. Lang also admitted using his cell phone number on the advertisements to coordinate the dates between the clients and the UJ. In addition, Lang goes to the dates with the UJ to provide protection. Lang receives monetary compensation from UJ for his role in the facilitation of the dates.

10. On September 15, 2016, an administrative subpoena was issued to Backpage.com for Internet Protocol (IP) records pertaining to the following Backpage.com Post ID's:

a. Post ID 18651242 tricities, dated August 29, 2016 10:58 pm

b. Post ID 18651308 tricities, dated August 29, 2016 11:05 pm

c. Post ID 18716697 tricities, dated September 10, 2016 7:36 pm

d. Post ID 18684956 tricities, dated September 11, 2016 7:44 pm

11. On September 19, 2016, Backpage.com responded, listing all IP addresses associated with the aforementioned Post IDs. Post ID 18684956, was posted on four separate dates, the first one being September 1, 2016, at 04:55:35 PM CDT. The IP address associated with that day and time was 76.23.88.104. IP address 76.23.88.104 belonged to Comcast Communications on that day and time.

12. On September 20, 2016, an administrative subpoena was issued to Comcast Communications for subscriber information pertaining to the person assigned IP address 76.23.88.104, on September 1, 2016, at 04:55:35 PM CDT.

13. On September 21, 2016, Comcast Communications responded to the aforementioned subpoena with the following subscriber information:

Subscriber Name:	Heather Lang
Service Address:	1108 Skyline Dr
	Johnson City, TN 37604
Telephone #:	423-557-7404
Type of Service:	High Speed Internet Service
Account Number:	8396514070144709
Account Status:	Active
IP Assignment:	Dynamically Assigned
E-mail User Ids:	hlang60, adamsjdavid
	(the above users ID(s) end in @comcast.net)

14. On September 13, 2016, your Affiant conducted an interview of Christopher Lang, brother of Brockett Lang. Christopher Lang reported that Brockett Lang had been living at 1108 Skyline Drive, Johnson City, TN, since the end of July 2016 and continued to live there until his arrest on September 12, 2016. Christopher Lang consented to a search of Brockett Lang's room. An initial search by your Affiant returned negative results for the Device. Approximately one hour later, Christopher Lang called your Affiant to report he found the Device in Brockett Lang's room under blankets in the closet. Christopher Lang turned the Device over to your Affiant.

15. The Device is currently in storage at the FBI Office located at 2620 Knob Creek Road, Johnson City, TN. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, [[and from consulting the manufacturer's advertisements and product technical specifications available online at www.hp.com, I know that the Device has capabilities that allow it to connect to the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

c. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

d. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

e. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

f. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

g. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

h. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

i. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

j. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review

team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

k. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

Bianca L. Pearson
Special Agent
FBI

Subscribed and sworn to before me
on October 5, 2016:

CLIFTON L. CORKER
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

The property to be searched is a Hewlett Packard Protect Smart Laptop computer, serial number 5CD4470XMM hereinafter the "Device." The Device is currently located at the FBI Johnson City Resident Agency 2620 Knob Creek Road, Johnson City, Tennessee, 37604.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Device described in Attachment A that relate to violations of Title 18 USC 1591(a)(1) and involve Brockett Patrick Ian Lang since August 20, 2016, including:

2. Records evidencing the use of the Internet Protocol address 76.23.88.104 to communicate with Backpage.com, including:

   a. records of Internet Protocol addresses used;

   b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.